

LE DIGITAL MARKETS ACT (DMA) – PARTIE I : LES OBLIGATIONS DES PLATEFORMES EN LIGNE

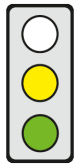
Analyse du cep du 28 juillet 2021

ÉLÉMENTS CLÉS

Contexte : Les plateformes numériques apportent des avantages aux utilisateurs et génèrent des opportunités commerciales. Toutefois, en raison de leur position entre les entreprises utilisatrices et les utilisateurs finaux, quelques grandes plateformes (« gatekeepers » ou « contrôleurs d'accès ») jouissent d'un pouvoir de marché important qui leur permet de capitaliser sur la dépendance économique et de limiter les possibilités d'entrée sur le marché pour les concurrents.

Objectif de la réglementation : Le Digital Markets Act (DMA – « loi sur les marchés numériques » en français) vise à garantir que les concurrents puissent entrer sur les marchés numériques et que les relations entre les contrôleurs d'accès et leurs utilisateurs soient équitables. À cette fin, le DMA contient des obligations pour les fournisseurs de services de plateforme [décrites dans cette **Analyse** du cep] ainsi que des règles d'application et de gouvernance [**Partie II** à suivre].

Acteurs concernés : Tous les utilisateurs finaux et les entreprises utilisatrices des contrôleurs d'accès et de leurs fournisseurs.



Pro : (1) Les seuils quantitatifs – c'est-à-dire ceux de chiffres d'affaires et/ou de capitalisation – déclenchent presque automatiquement l'application du DMA. Cette applicabilité directe de toutes les obligations permet une mise en œuvre rapide.

(2) Dans l'ensemble, les obligations imposées aux contrôleurs d'accès sont appropriées.

Contra : Le manque de précision concernant les conditions préalables à ce que la Commission puisse déclarer qu'une entreprise est un contrôleur d'accès bien qu'elle n'atteigne pas les seuils quantitatifs est problématique eu égard au principe de sécurité juridique. Des lignes directrices sur la manière dont la Commission peut procéder à une telle évaluation sont nécessaires.

Les passages les plus importants du texte sont mis en évidence par une ligne dans la marge.

CONTENU

Titre

Proposition COM(2020) 842 du 15 décembre 2020 pour un **règlement relatif aux marchés contestables et équitables dans le secteur numérique.**

Fiche technique

► Contexte et objectifs

- Le Digital Markets Act (DMA, « loi sur les marchés numériques » en français) vise à faire en sorte que les marchés numériques restent contestables et équitables en imposant des règles de conduite strictes à certains fournisseurs de « services de plateforme essentiels » (SPE) définis comme des « gatekeepers » ou « contrôleurs d'accès ». Une entreprise est un fournisseur de SPE si elle fournit au moins l'un des services suivants [Art. 2 (2)] :
 - un service d'intermédiation en ligne, par exemple Amazon Marketplace, Apple App Store ;
 - un moteur de recherche en ligne, par exemple Google ;
 - un service de réseau social en ligne, par exemple Facebook ;
 - un service de plateforme de partage de vidéos, par exemple Youtube ;
 - un service de communication interpersonnelle non fondée sur la numérotation, par exemple Skype ;
 - un système d'exploitation, par exemple Android ou Windows ;
 - un service en nuage, par exemple Amazon Web Services ; ou
 - un service de publicité, si le prestataire offre également au moins un des SPE mentionnés ci-dessus.
- La proposition du DMA contient
 - des obligations pour certains fournisseurs de SPE [la présente **Analyse** du cep] et
 - les règles d'application et de gouvernance [**Partie II** à suivre].

► **Contrôleurs d'accès**

- Un « contrôleur d'accès » est un prestataire de SPE qui répond aux critères suivants [Art. 3 (1), (2)] :
 - Il a un poids important sur le marché intérieur, ce qui est postulé si la plateforme fournit un SPE dans au moins trois États membres et :
 - que son chiffre d'affaires annuel dans l'Espace économique européen au cours des trois dernières années était supérieur ou égal à 6,5 milliards d'euros ou
 - que sa capitalisation boursière moyenne au cours du dernier exercice était supérieur ou égale à 65 milliards d'euros.
 - Il exploite un SPE qui sert de passerelle importante permettant aux entreprises utilisatrices d'atteindre les utilisateurs finaux, ce qui est postulé si le SPE compte dans l'UE plus de 45 millions d'utilisateurs finaux actifs par mois et plus de 10 000 entreprises utilisatrices actives par an.
 - Il bénéficie d'une position solide et durable dans la fourniture d'un SPE ou il est prévisible qu'il bénéficiera d'une telle position dans un avenir proche, ce qui est postulé si les critères énoncés au tiret précédent ont été remplis au cours de chacun des trois derniers exercices.
- Un fournisseur de SPE qui atteint les seuils quantitatifs doit en informer la Commission [Art. 3 (3)].
- La Commission doit déclarer que le prestataire est un contrôleur d'accès, à moins que ce prestataire ne démontre que, bien qu'il respecte les seuils quantitatifs, il ne remplit pas les critères préalables [Art. 3 (4), (6)].
- Les indicateurs pertinents permettant de montrer qu'il est un contrôleur d'accès comprennent la taille du fournisseur de SPE et les barrières à l'entrée pour les concurrents.
- Sur la base, entre autres, de ces indicateurs, la Commission peut, après une enquête de marché, déclarer qu'un fournisseur est un contrôleur d'accès s'il remplit les critères inhérents à ce statut sans atteindre les seuils quantitatifs [Art. 3, § 6 ; considérant 25].
- Les obligations des contrôleurs d'accès ne s'appliquent qu'aux SPE pour lesquels ils remplissent les critères de contrôleurs d'accès [Art. 5, Art. 6].

► **Obligations des contrôleurs d'accès [Art. 5]**

- Les contrôleurs d'accès doivent [Art. 5 (a)-(g)] :
 - s'abstenir, à moins que l'utilisateur final n'y consente,
 - de combiner les données personnelles obtenues par le biais du SPE avec des données personnelles provenant de tout autre service du contrôleur d'accès ou avec des données personnelles provenant de services tiers ;
 - d'inscrire automatiquement des utilisateurs finaux à d'autres services dudit contrôleur d'accès afin de combiner les données personnelles ;
 - permettre
 - aux entreprises utilisatrices d'offrir les mêmes services aux utilisateurs finaux par le biais de services d'intermédiation en ligne tierces, à des conditions différentes de celles offertes par les services d'intermédiation du contrôleur d'accès ;
 - aux entreprises utilisatrices de faire des offres aux utilisateurs finaux acquis par le biais du SPE et de conclure des contrats avec ces derniers, que ces contrats soient ou non conclus en utilisant le SPE du contrôleur d'accès, et
 - aux utilisateurs finaux de pouvoir accéder à et utiliser, par le biais du SPE du contrôleur d'accès, des services – tels que les applications – obtenus en dehors du SPE du contrôleur d'accès ;
 - s'abstenir d'empêcher les entreprises utilisatrices de porter plainte auprès des autorités publiques des pratiques des contrôleurs d'accès ;
 - s'abstenir d'exiger des entreprises utilisatrices qu'elles utilisent, offrent ou interagissent avec un service d'identification du contrôleur d'accès ;
 - s'abstenir d'exiger des utilisateurs du SPE qu'ils s'inscrivent ou s'abonnent à un autre SPE qui est géré par un contrôleur d'accès ou qui compte dans l'UE plus de 45 millions d'utilisateurs finaux actifs chaque mois et plus de 10 000 entreprises utilisatrices actives chaque année ; et
 - fournir aux annonceurs et aux éditeurs – c'est-à-dire à ceux qui fournissent des espaces publicitaires – sur leur demande des informations concernant le prix payé par l'annonceur et l'éditeur pour les services publicitaires du contrôleur d'accès et la rémunération versée à l'éditeur pour la publication d'une annonce donnée.

► **Obligations des contrôleurs d'accès susceptibles d'être précisées ultérieurement par la Commission [Art. 6, Art. 7]**

- Les contrôleurs d'accès doivent [Art. 6 (1) (a)-(k)]
 - s'abstenir d'utiliser – lorsqu'ils sont en concurrence avec des entreprises utilisatrices de son SPE – toute donnée non disponible publiquement générée par les activités de ces entreprises utilisatrices ou fournie par ces entreprises utilisatrices ou leurs utilisateurs finaux ;
 - permettre aux utilisateurs finaux de désinstaller les applications préinstallées sur leurs SPE ;
 - permettre l'installation et l'utilisation effective d'applications émanant de tierces instances et des « app stores » (boutiques d'applications en français) en ligne qui utilisent ou interagissent avec leur système

- d'exploitation et permettre l'accès à ces applications et à ces app stores par d'autres moyens que l'app store du système d'exploitation ;
 - s'abstenir de traiter ses propres services plus favorablement que les services similaires de tiers lors de leur classement, et appliquer des conditions équitables et non discriminatoires à ces classements ;
 - s'abstenir de restreindre techniquement la capacité des utilisateurs finaux à passer d'une application et d'un service à l'autre et à s'y abonner par le biais de leur système d'exploitation ;
 - permettre aux entreprises utilisatrices et aux fournisseurs de services auxiliaires, par exemple aux services d'identification ou de paiement, d'accéder au système d'exploitation, au matériel ou aux logiciels utilisés par les services auxiliaires des contrôleurs d'accès et d'assurer l'interopérabilité avec ceux-ci ;
 - fournir aux annonceurs et aux éditeurs, sur demande et gratuitement, un accès aux outils de mesure de la performance du contrôleur d'accès et aux informations nécessaires pour effectuer leur propre vérification de l'endroit où l'annonce a été affichée ;
 - fournir une portabilité effective, continue et en temps réel des données générées par l'activité d'une entreprise utilisatrice ou d'un utilisateur final, notamment avec des outils destinés aux utilisateurs finaux pour faciliter l'exercice de la portabilité des données ;
 - fournir gratuitement aux entreprises utilisatrices un accès efficace, de haute qualité, continu et en temps réel aux données qui sont fournies pour ou générées par ces entreprises utilisatrices et leurs utilisateurs finaux dans le cadre de l'utilisation du SPE et leur permettre d'utiliser ces données ;
 - fournir un accès à tout fournisseur tiers de moteurs de recherche en ligne, à des conditions équitables, raisonnables et non discriminatoires, aux données de classement, de requêtes, de clics et de vues qui ont été générées par les utilisateurs finaux sur les moteurs de recherche en ligne du contrôleur d'accès ;
 - appliquer, enfin, des conditions générales d'accès équitables et non discriminatoires aux app stores pour les entreprises utilisatrices.
- À la suite d'un dialogue avec le contrôleur d'accès concerné, la Commission peut préciser les mesures que celui-ci doit prendre pour assurer le respect effectif de ces obligations [Art. 7, § 2].

► **Applicabilité des règles et obligations d'information**

- Si le respect d'une obligation spécifique risque, en raison de circonstances exceptionnelles, de compromettre la viabilité économique d'un contrôleur, la Commission peut, sur demande, suspendre une obligation spécifique (Art. 8).
- Les contrôleurs d'accès doivent informer la Commission de tout projet de fusion ou d'acquisition impliquant un autre fournisseur de services numériques [Art. 12 (1)].

Déclaration de la Commission sur la subsidiarité

Les acteurs numériques, notamment ceux visés par le DMA, opèrent généralement dans un contexte international. Ainsi, les problèmes à résoudre sont transfrontaliers et concernent plusieurs États membres.

Contexte politique

Le DMA s'appuie sur les consultations de la Commission sur le « nouvel outil de concurrence » et sur « l'instrument de régulation ex ante des très grandes plateformes en ligne jouant le rôle de contrôleurs d'accès » (voir [Input du cep](#)). Avec le [Digital Services Act](#) (voir [Étude du cep](#); [Analyse du cep](#) à suivre), publié le même jour, le DMA fait partie de la proposition de la Commission sur la nouvelle réglementation sur les plateformes numériques.

Procédure législative

Adoption par la Commission	15 décembre 2020
Adoption par le Parlement européen et le Conseil, publication au Journal officiel de l'Union européenne, entrée en vigueur	en cours

Options pour influencer le processus politique

Directions générales :	DG Réseaux de communication, contenu et technologie
Commissions du Parlement européen :	IMCO (compétente), Rapporteur : Andreas Schwab (Groupe PPE, Allemagne)
Mode de prise de décision au Conseil :	Majorité qualifiée (55 % des États membres représentant 65 % de la population de l'UE).

Formalités

Compétence :	Art. 114 du TFUE (marché intérieur)
Type de compétence législative :	Compétence partagée (art. 4 (2) TFUE)
Procédure :	Art. 294 TFUE (procédure législative ordinaire)

ÉVALUATION

Évaluation économique

D'une part, plus le fournisseur de SPE est important – c'est-à-dire plus il offre de produits et de services par le biais d'un service d'intermédiation et plus il compte d'utilisateurs – plus il répond efficacement à la demande, ce qui amène encore plus d'utilisateurs à adhérer au SPE par ce qui est communément appelé un « effet de réseau ». D'autre part, cet effet de réseau peut permettre à un fournisseur de SPE de dominer le marché. **Le pouvoir qui en résulte pour le fournisseur de SPE peut être utilisé pour** augmenter les prix, décourager l'innovation et **empêcher l'entrée sur le marché de concurrents** (pour plus de détail sur ce point, voir l'[Input du cep](#)). **L'objectif du DMA de garantir la contestabilité et l'équité** – c'est-à-dire d'éviter l'exploitation de la dépendance économique – **des marchés numériques, est donc approprié.**

La qualification de contrôleur d'accès est à juste titre fondée sur des **seuils quantitatifs** qui **déclenchent presque automatiquement l'application du DMA. Avec l'applicabilité directe de toutes les obligations, leur mise en œuvre est rapide**, ce qui contribue à garantir la contestabilité des marchés numériques, en empêchant certains comportements qui limiteraient la concurrence ou exploiteraient la dépendance économique des entreprises. Il est important d'agir ainsi ex-ante car les remèdes ex-post peuvent être inefficaces, notamment s'ils prennent tellement de temps qu'il ne reste plus d'agents économiques autre que le contrôleur d'accès sur le marché. **Dans l'ensemble, les obligations imposées aux contrôleurs d'accès sont équilibrées**, car elles s'attaquent à des comportements problématiques qui font souvent l'objet d'enquêtes en vertu du droit de la concurrence, sans peser excessivement sur leurs autres pratiques, jugées bénéfiques. Il est approprié d'avoir deux listes d'obligations. Bien que toutes les obligations soient directement applicables, la Commission offre des conseils sur la manière de se conformer aux obligations auxquelles il est jugé plus difficile de se conformer, qui sont énoncées à l'Art. 6. C'est particulièrement vrai lorsqu'elles impliquent différentes méthodes de mise en conformité, notamment en raison du modèle économique du contrôleur d'accès. De telles orientations peuvent éviter d'imposer des obligations qui, autrement, seraient trop lourdes ou techniquement impossibles à respecter.

En ce qui concerne les obligations sélectionnées, le fait de permettre aux entreprises utilisatrices d'offrir le même service à des conditions différentes sur d'autres plateformes empêche un contrôleur d'accès d'exploiter la dépendance économique des entreprises utilisatrices opérant sur son SPE, par exemple, via des clauses de parité étendue. L'interdiction d'exiger que les utilisateurs d'un SPE s'inscrivent ou s'abonnent à un autre SPE empêche les contrôleurs d'accès de lier leurs services, ce qui réduirait la contestabilité sur les marchés adjacents existants ou émergents. Cependant, les seuils quantitatifs de 45 millions d'utilisateurs finaux actifs par mois et de plus de 10 000 entreprises utilisatrices actives par an sont trop élevés car ils ne tiennent pas compte de la capacité des contrôleurs d'accès à tirer parti de leur pouvoir de marché à partir de leur SPE vers un service où leur pouvoir de marché est limité. Les obligations d'autoriser l'installation d'applications et d'app stores tiers et de permettre l'interopérabilité des services auxiliaires sur des systèmes et matériels opérationnels empêchent un contrôleur d'accès d'interdire à un concurrent d'entrer sur le marché, par exemple en lui refusant l'accès à son propre app store, ce qui renforce la concurrence. Ces obligations sont essentielles au bon fonctionnement du reste des dispositions. Par exemple, alors qu'il est approprié de permettre aux utilisateurs finaux de désinstaller les applications préinstallées, dans le cas où aucun concurrent ne peut remplacer l'application du contrôleur d'accès, les utilisateurs n'ont d'autre choix que d'utiliser son application.

Évaluation juridique

Compétence législative de l'UE

Le DMA est fondé à juste titre sur la compétence du marché intérieur (art. 114 TFUE).

Subsidiarité et proportionnalité à l'égard des États membres

Non pertinent, puisque les contrôleurs d'accès, par définition, opèrent de manière transfrontalière.

Compatibilité avec le droit communautaire à d'autres égards

Les obligations imposées aux contrôleurs d'accès portent atteinte à la liberté d'entreprise [Art. 16 de la Charte des droits fondamentaux de l'Union européenne (CDF)]. Toutefois, pour les raisons exposées dans l'évaluation économique, l'interférence avec la liberté d'entreprise sert un objectif légitime – assurer la contestabilité et l'équité des marchés numériques – et le fait de manière appropriée. Notamment, les seuils quantitatifs sont suffisamment élevés pour ne concerner que les plus grands fournisseurs de SPE, de sorte que le DMA n'affecte pas les petites entreprises. Il n'y a pas d'atteinte à l'Art. 16 de la Charte des Droits Fondamentaux.

Toutefois, **le manque de précision concernant les circonstances dans lesquelles la Commission peut déclarer qu'une entreprise est un contrôleur d'accès bien qu'elle n'atteigne pas les seuils quantitatifs est problématique en raison de l'atteinte portée au principe de sécurité juridique.** Bien que la flexibilité juridique soit nécessaire dans une économie numérique qui évolue rapidement, des **lignes directrices définissant la manière dont la Commission peut**

procéder à une telle évaluation sont nécessaires. Il convient notamment de clarifier si la Commission peut déclarer que les petits fournisseurs de SPE ancrés dans des marchés de niche sont des contrôleurs d'accès.

Le DMA et le Règlement général sur la protection des données (RGPD) ont des objectifs différents : l'objectif du DMA est de garantir des marchés numériques contestables et équitables, tandis que celui du RGPD est d'harmoniser la protection des données personnelles des personnes physiques, garantissant ainsi la libre circulation des données personnelles au sein de l'UE. Pour cette raison, le DMA complète et va au-delà du RGPD. Contrairement à l'art. 20 du RGPD, le droit à la portabilité des données du DMA [Art. 6 (1) (h)] couvre les données des entreprises et des utilisateurs finaux, que l'utilisateur soit ou non une personne physique. En outre, alors que le RGPD prévoit simplement un droit de recevoir ses propres données personnelles dans un format structuré, couramment utilisé et lisible sur un terminal informatique, le DMA offre un droit d'accès continu et en temps réel aux données personnelles. En outre, en interdisant la combinaison de données à caractère personnel provenant de différents services sans consentement des utilisateurs finaux [Art. 5 (a)], le DMA va également au-delà du RGPD, qui prévoit des motifs supplémentaires rendant le traitement des données licite, tels que les intérêts légitimes du responsable du traitement.

Résumé de l'évaluation

Le pouvoir du fournisseur de SPE pourrait être utilisé pour entraver l'entrée des concurrents sur le marché. L'objectif du DMA de garantir la contestabilité et l'équité sur les marchés numériques est donc approprié. Les seuils quantitatifs déclenchent presque automatiquement l'application du DMA. Outre l'applicabilité directe de toutes les obligations, cela permet sa mise en œuvre rapide. Dans l'ensemble, les obligations imposées aux contrôleurs d'accès sont équilibrées. Le manque de précisions concernant les circonstances dans lesquelles la Commission peut déclarer qu'une entreprise est un contrôleur d'accès bien qu'elle n'atteigne pas les seuils quantitatifs, est problématique au regard du principe de sécurité juridique. Des lignes directrices définissant la manière dont la Commission peut procéder à une telle évaluation sont nécessaires.